SUBJ: INTERNET ACCESS POINTS

1. **PURPOSE.** This order serves as an implementation directive to Order 1370.82, Information Systems Security Program, prescribing responsibilities and identifying procedures for establishing and operating an agency Internet Access Point (IAP). Additionally, this order establishes an Internet Access Point Configuration Control Committee (IAP CCC).

2. **DISTRIBUTION.** This order is distributed to the division level in Washington headquarters, regions, and centers and a limited distribution to all field offices and facilities.

3. **SCOPE.**

   a. This order applies to all offices, services, regions, centers, employees, contractors, support personnel, and all others who use Federal Aviation Administration (FAA) systems, applications, data, information, and other resources, including those entities identified in Order 1370.82, Information Systems Security Program. This order also applies to all systems, including National Airspace Systems (NAS), devices, networks, and applications that establish a connection to the Internet or use Internet resources with the exception of mobile Internet access, i.e., laptops, personal digital assistants, cellular phones, pagers, etc., which will be addressed in future guidance. This order applies to all existing and future FAA Internet connections. NAS system owners that require an Internet connection shall justify their Internet connection in the current security certification and authorization package (SCAP) for that system in accordance with Order 1370.82. Additionally, if that connection is to be via an IAP that is not currently approved in accordance with this order, then the use of the IAP shall also be justified in accordance with this order.

   b. This order ensures that the availability, integrity, and confidentiality of FAA resources are maintained and that individuals and organizations are accountable for the use of IAP services. In addition, this order introduces a practical and feasible process that enables the FAA to manage the configuration of IAP's from a central point through a cooperative effort between the Designated Approving Authority (DAA) and the Assistant Administrator for Information Services and Chief Information Officer (AIO-1).

4. **BACKGROUND.** Order 1370.82, Information Systems Security Program, states that AIO-1 is authorized to issue detailed information systems security (ISS) implementation orders, procedures, and guidance. The FAA currently provides Internet access to its employees and on-site contractors through arrangements with commercial Internet Service Providers through one of eight recognized IAP's. As specified in Order 1370.79A, Internet Use Policy, four of the recognized IAP locations are Washington headquarters, Information Technology Division (ASU-500); Mike Monroney Aeronautical Center, Office of Information Services (AMI-1); Western-Pacific Region, Financial and Management Resources Division (AWP-40); and the William J. Hughes Technical Center, Office of the Director (ACT-1). Due to the increased use and dependency of the Internet throughout the agency, three additional IAP's have been recognized: Eastern Region, Flight Standards Division (AEA-200); Great Lakes Region, Information Technology Services (AGL-40); and Alaskan Region, Resource Management Division (AAL-40); as specified in paragraph 7.a. Due to an existing agreement between the Department of Transportation/FAA and the Department of Defense, an IAP operated by ASU-500 located at the Air Traffic Control Systems Command Center (ATCSCC) in Herndon, Virginia, is also recognized.

5. **ACTION.** This order contains actions required to be completed by a specific date.

   a. All currently recognized IAP's shall be certified and authorized by September 30, 2001, or cease to operate.

b. For any other existing IAP's, a justification paper shall be submitted to AIO and the relevant DAA within 45 days of the approval date of this order. Paragraph 7.b. contains additional guidance on the justification process.

(1) If the IAP justification paper is approved by the DAA and AIO-1, the IAP shall be certified and authorized by September 30, 2001, or cease to operate.

(2) If the justification paper is disapproved by the DAA and AIO-1, the IAP shall cease to operate by September 30, 2001.

c. The Director of Information Systems Security (AIS-1) or his/her designee shall hold the first meeting of the IAP CCC within 30 days after approval of this order (see paragraph 8).

d. Within 90 days of the approval date of this order, the IAP CCC will:

(1) Prepare and submit the IAP CCC charter to AIO-1 for approval.

(2) Brief AIO-1 on IAP CCC role.

6. DEFINITIONS. Appendix 1, Definitions, defines the terms used in this order.

7. PROCEDURES. In accordance with Order 1370.82, Information Systems Security Program, and due to the increased emphasis on information security, this order requires that all IAP's be certified and authorized to ensure their secure operation. All guidance to prepare a SCAP is contained in the Information Systems Security Enhancement Program Handbook, dated September 2000 or subsequent versions, which was distributed to each line of business/staff office. This handbook provides a framework for the various organizations within the FAA to develop programs for enhancing their ISS and provides direction regarding the types of information to be collected and documented, the assessment of that information, and a process for ISS certification and authorization. Should an IAP not maintain compliance with this order, AIS will give the IAP sponsoring organization 30 days to comply. Failure to comply within 30 days will result in decertification and, subsequently, the IAP shall cease to operate.

a. Recognized IAP's. There are currently eight recognized IAP's in use by the agency: Washington headquarters (ASU-500), Mike Monroney Aeronautical Center (AMI-1), Western-Pacific Region (AWP-40), William J. Hughes Technical Center (ACT-1), Eastern Region (AEA-200), Great Lakes Region (AGL-40), Alaskan Region (AAL-40), and Herndon ATCSCC (ASU-500). A SCAP for each of these IAP's shall be submitted to AIS-1 and the relevant DAA for certification and authorization. Each IAP shall be certified and authorized by September 30, 2001, or cease to operate.

b. Other Existing IAP's. Any office, service, region, or center that manages an IAP beyond the eight currently recognized IAP's shall submit a justification paper containing a clear, concise justification statement as to why this IAP is required and rationale as to why a recognized IAP cannot be used. Since the cost and difficulty of ensuring FAA ISS increases nonlinearly with the addition of IAP's, the number of IAP's will be limited. The justification paper shall be submitted to AIO-1 and the relevant DAA for approval within 45 days of the signature date of this order. If the justification paper is approved, a SCAP shall be prepared and submitted by the IAP sponsoring organization, approved by AIS-1, and the IAP shall be certified and authorized by September 30, 2001, or cease to operate. If the justification paper is disapproved, the IAP shall cease to operate by September 30, 2001.

c. New IAP's. To establish a new IAP, a justification paper shall be submitted to and approved by AIO-1 and the appropriate DAA, and the IAP must be certified and authorized prior to beginning operations. NAS system owners that utilize an Internet connection shall specify this in the SCAP for that NAS system. If that connection is not via one of the eight recognized IAP's, then requirements for establishing a new IAP shall be followed in accordance with this order.

d. Waiver. Waivers, extensions, and other exceptions to these procedures may be granted by AIO-1 when special circumstances permit.

8. IAP CONFIGURATION CONTROL COMMITTEE.

a. AIS-1 will hold the first meeting of the IAP CCC within 30 days after approval of this order. Within 90 days of the approval date, the IAP CCC shall prepare its charter, specify how it will participate in implementing this order, and brief

AIO-1 on its recommendations. AIS-1 or his/her designee will chair the IAP CCC. The IAP CCC will be composed of Federal employees associated with each recognized IAP and representatives from the ATS, ARA, ARC, AVR, ACS, ARP, and ASY lines of business and the Enterprise Network and Computer Security Incident Response Capability (CSIRC) offices.

    b.   The IAP CCC will provide guidance for all issues relating to IAP configuration management and access to FAA systems and resources.

    c.   The IAP CCC will perform comprehensive reviews of IAP justification papers and review requests for deviation from IAP standards.

    d.   The IAP CCC will make recommendations on network, hardware, and software requirements; equipment standards; component configurations; and protocols and services authorized at each IAP. However, operational activities, such as implementation of configuration changes, modifications of IAP systems and devices, system and software upgrades, and access control, will be performed locally.

9.   **ROLES AND RESPONSIBILITIES**. The FAA will provide a secure IAP for those FAA employees and support contractors whose management deems it a business requirement. AIO shall manage the number, location, and configuration of the IAP's to ensure adequate security, reasonable cost, and efficient operation.

    a. Office of Information Services and Chief Information Officer (AIO).

        (1)   Assistant Administrator for Information Services and Chief Information Officer (AIO-1).

            (a)   Approves, denies, or terminates IAP's with the concurrence of the relevant DAA.

            (b)   Approves IAP justification papers with the concurrence of the relevant DAA.

            (c)   Ensures all offices, services, regions, centers, employees, contractors, support personnel, and all others who use FAA systems, applications, data, information, and other resources to include entities identified in Order 1370.82, Information Systems Security Program, comply with this IAP order.

            (d)   Ensures adherence to 1370.79A, Internet Use Policy.

        (2)   Director of Information Systems Security (AIS-1).

            (a)   Develops agency IAP standards and guidance.

            (b)   Chairs the IAP CCC activities and provides oversight of all IAP's security.

            (c)   Certifies IAP's based upon review of SCAP.

            (d)   Monitors and ensures compliance with this order.

    b. Designated Approving Authority (DAA).

        (1)   Approves, denies, or terminates IAP's with the concurrence of AIO-1.

        (2)   Approves the justification paper and forwards to AIO-1 for concurrence.

        (3)   Authorizes IAP's based on review of the SCAP and certification from AIS-1.

    c. Office of Acquisitions (ASU).

        (1)   Serves as the primary advisor to the IAP CCC on technical issues.

        (2)   Assists the IAP CCC in establishing and reviewing security configuration standards, policies, and practices.

(3) Maintains all public and private FAA Internet Protocol addresses.

(4) Informs the IAP CCC of new and existing hardware and software configurations, services, and components.

d. CSIRC Office.

(1) Processes all reports of computer security incidents against FAA IAP's.

(2) Installs, operates, and maintains intrusion detection systems (IDS) at the IAP's.

(3) Provides the local IAP administrators with access to IDS data relative to their IAP.

e. IAP Sponsoring Organization.

(1) Staffs, funds, and operates the IAP.

(2) Develops an IAP justification paper and submits it to AIO-1 and the relevant DAA for approval.

(3) Prepares a SCAP for the IAP and provides documentation to both AIS-1 and the relevant DAA for review and proposed certification and authorization.

f. IAP Administrators and Operational Support.
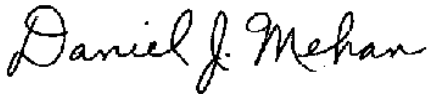
(1) Performs day-to-day operations of the IAP.

(2) Implements IAP guidance.

(3) Provides IAP information to the IAP CCC upon request.

(4) Analyzes log files, performs traffic analysis, collects and maintains statistics on IAP use and activity.

(5) Reports ISS incidents immediately to the CSIRC.

(6) Provides the CSIRC with access to all appropriate IAP log files, statistics, traffic analysis, and incident data in a timely manner.

Daniel J. Mehan
Assistant Administrator for Information Services
    and Chief Information Officer

APPENDIX 1. DEFINITIONS

Accountability. The quality or state that enables violations or attempted violations of ISS to be traced to individuals who may then be held responsible.

Availability. Timely, reliable access to data and information services for authorized users.

Certification and Authorization (C&A). A set of processes and procedures by which the security posture of an information system is reviewed for the inclusion of adequate security measures and the decision about whether to authorize the system for operation.

Confidentiality. A requirement that private or confidential information not be disclosed to unauthorized individuals.

Configuration Control Committee (CCC).   A committee designed to provide guidance for all issues relating to IAP configuration management and access to FAA systems and resources, perform comprehensive reviews of IAP justification papers, and review requests for deviation from IAP standards. This committee also makes recommendations on network, hardware, and software requirements; equipment standards; component configurations; and protocols and services authorized at each IAP.

Designated Approving Authority (DAA). A senior FAA management official, appointed in writing by a member of the Management Board, who determines whether or not to authorize a system for operation or to remove that authorization.

Integrity. A requirement that information and programs are changed only in a specified and authorized manner and that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

Internet. A global network of independent hosts and communications facilities, which connect users to those hosts. The term "Internet" also may refer to the content presented on the hosts or transmitted through the network. The FAA may contribute information and resources to the Internet for public consumption.

Internet Access. The connection to the public Internet or access to any Internet resource or information using any application, program, software, utility or tool, for any reason or duration. For the purpose of this document, Internet access includes any permanent or temporary connection to the Internet.

Internet Access Point (IAP). Any physical or logical connection to the public Internet. An IAP includes any direct or permanent connection or any dial-up or temporary connection to the Internet.

Internet Service Provider (ISP). The connection point or organization outside the FAA, connected either physically or logically to an IAP, that is the means by which the IAP gains access to the Internet.

Intranet. The FAA's internal or private network used to share information and resources within the FAA community. Information and resources on the Intranet are not made available to the public.

Management Board. A board chaired by the Administrator, and the membership consists of the Deputy Administrator, Assistant and Associate Administrators, and Chief Counsel.

National Airspace System (NAS). The common network of U.S. airspace; air navigation facilities, equipment and services, airports or landing areas; aeronautical charts, information and services; rules, regulations and procedures; technical information; and human resources and material. Included are system components shared jointly with the military.

Network. Communications hardware and software that allow one user or system to connect to another user or system and can be part of a system or a separate system. Examples include local area networks (LAN's) and wide area networks (WAN's) and public networks such as the Internet.

Security Certification and Authorization Package (SCAP). The package that is presented to the DAA for final authorization of the IAP. The SCAP includes the ISS plan, vulnerability assessment report, risk assessment, security test plan and results, disaster recovery and contingency measures, and ISS C&A statements.